TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/08/2016

SUBJECT:
Multiple Vulnerabilities in Windows Media Could Allow Remote Code Execution (MS16-027)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Windows Media which could allow remote code execution. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Windows 7
- Windows 8.1, RT 8.1
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012, 2012 R2

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Two vulnerabilities exist in Windows Media, which could allow for remote code execution (CVE-2016-0098 and CVE-2016-0101). These vulnerabilities exist due to how Windows Media handles resources in the media library. In order to exploit these vulnerabilities an attacker would have to convince a user to open a specially crafted email attachment, or visit an untrusted webpage hosting the specially crafted media content. Successful exploitation of these vulnerabilities could result in an attacker gaining the

same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Microsoft:
https://technet.microsoft.com/en-us/library/security/ms16-027.aspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0098
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0101

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/